Jméno: _____ Datum: _____ Body: _____

Prevence krádeže identity a majetek Průvodce zabezpečením

Úniky přihlašovacích údajů, MFA, monitorování dark webu, upozornění na zmrazení úvěru, sociální inženýrství

PŘEHLED VÝUKY: PREVENCE KRÁDEŽE IDENTITY

ZABEZPEČENO
ŠIFROVÁNÍ DAT
Standard 256bitového AES

VYHOVUJÍCÍ
GLOBÁLNÍ STANDARDY
Rámce GDPR a CCPA

ZERO-TRUST
ZÁSADY PŘÍSTUPU
Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede prevencí a zmírňováním krádeží identity. Prozkoumáte úniky přihlašovacích údajů, vícefaktorové ověřování, monitorování dark webu, upozornění na zmrazení úvěru a obranu proti sociálnímu inženýrství.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/kradez-identity/

Váš studijní plán: ochrana identity

- Pochopte rizika odhalení přihlašovacích údajů na fórech dark webu.
- Zavést vícefaktorovou autentizaci (MFA) a upozornění na zmrazení úvěru.
- Navrhněte firemní bezpečnostní obranu proti cíleným podvodům sociálního inženýrství.

POKYNY K PRŮVODCI KRÁDEŽÍ IDENTITY

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na ochranu identity. Zakončete bonusovou aktivitou Mysli rychle.

PREVENCE KRÁDEŽE IDENTITY A ZABEZPEČENÍ MAJETKU (ÚVOD)

Krádež identity zneužívá uniklé přihlašovací údaje a slabá přihlášení k ovládnutí osobních i firemních účtů. Nasazení MFA, zmrazení úvěru, skenerů temného webu a rámců SPF/DKIM/DMARC tvoří klíčovou obranu proti digitálnímu vydávání se za někoho jiného.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU ODPOVĚĎ.

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Jakou primární metodu používají zloději identity ke krádeži přihlašovacích údajů?

- A. Rozesílání falešných e-mailových upozornění, která uživatele přimějí zadat hesla na podvržených portálech
- B. Poslech rozhlasového vysílání poblíž firemní kanceláře uživatele
- C. Defragmentace místního úložného disku serveru uživatele
- D. Odpojení externích síťových záloh

2. Jaká bezpečnostní kontrola poskytuje nejsilnější obranu proti únikům přihlašovacích údajů?

- A. Vícefaktorová autentizace pomocí hardwarových klíčů
- B. Vytváření dlouhých hesel pomocí výchozích formátů prohlížeče
- C. Změna e-mailových uživatelských jmen každých šest měsíců
- D. Mazání uložených historií sledovacích cookies v prohlížeči

3. Co představuje zmrazení úvěru?

- A. Uzamčení úvěrových zpráv, aby zloději nemohli sjednávat neautorizované půjčky
- B. Mazání historií bankovních transakcí z databází
- C. Deaktivace čteček magnetických proužků kreditních karet na skenerech
- D. Šifrování místních databázových disků v klidovém stavu

4. Proč je monitoring dark webu užitečný?

- A. Upozorní uživatele, pokud se jejich uniklé přihlašovací údaje objeví v nelegálních databázích
- B. Brání spuštění aktivního malwaru ve virtuálních sandboxech
- C. Zrychluje směrování prohlížeče ve virtuálních sítích
- D. Blokuje pokusy o přístup přes SQL injection do backendové databáze

5. Co znamená sociální inženýrství?

- A. Manipulace lidí, aby dobrovolně vyzradili důvěrné přihlašovací údaje
- B. Skenování portů firemních serverů kvůli aktivním zneužitím
- C. Zálohování systémových databázových souborů na offline pevné disky
- D. Směrování síťových paketů přes tři šifrované onion uzly

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka 6

6. Krádež identity se týká pouze online digitálních účtů, ne fyzické poštovní korespondence.

- ○ Pravda
- ○ Nepravda

7 Otázka 7

7. Vynucení MFA na všech osobních účtech blokuje většinu botových útoků typu credential stuffing.

- ○ Pravda
- ○ Nepravda

8 Otázka 8

8. Zmrazení úvěru blokuje úvěrové kontroly, ale brání vám v přístupu k vlastnímu bankovnímu účtu.

- ○ Pravda
- ○ Nepravda

9 Otázka 9

9. Správci hesel chrání uživatele před phishingem tím, že odmítají automaticky vyplňovat hesla na podvržených doménách.

- ○ Pravda
- ○ Nepravda

10 Otázka 10

10. Phishingové e-maily často používají naléhavý jazyk, aby vyvolaly emotivní, rychlé reakce.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Zloději identity se snaží získat uživatelská jména, hesla a další _____ .

2. Soukromé údaje o účtech odhalují databázové _____ , na které služby uživatele upozorňují.

3. Vyžadování dočasného kódu při přihlášení se označuje zkratkou _____ .

4. Prohledávání hackerských fór kvůli ukradeným datům se nazývá _____ dark webu.

5. Neoprávněné úvěrové kontroly blokuje úvěrové _____ .

6. Školením zaměstnanců v rozpoznávání phishingu vzniká aktivní bezpečnostní _____ .

ZÁSOBNÍK SLOV

MFA MONITOROVÁNÍ OBRANA PHISHING PŘIHLAŠOVACÍ ÚDAJE SPOOFING ÚNIKY ZMRAZENÍ

Sem napište své odpovědi:

1. **2.**

3. **4.**

5. **6.**

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

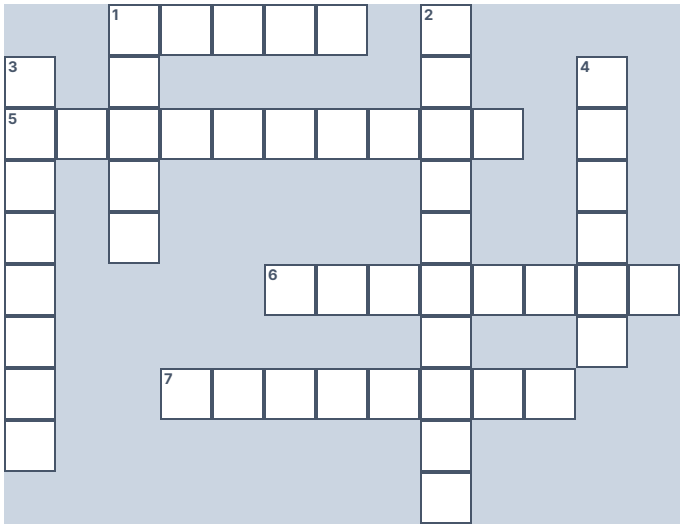
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. PŘIHLAŠOVACÍ ÚDAJE	A	Sekundární ověřovací krok (například hardwarové klíče) chránící přihlášení k účtům.
☐	2. ÚNIKY	B	Vytvoření falešného webu nebo e-mailu napodobujícího legitimní organizaci.
☐	3. MFA	C	Omezení přístupu k úvěrovým záznamům, aby se zabránilo podvodným žádostem o úvěr.
☐	4. MONITOROVÁNÍ	D	Neoprávněné odhalení soukromých databází obsahujících osobní záznamy uživatelů.
☐	5. ZMRAZENÍ	E	Školení a technická opatření používaná k ochraně před krádeží identity.
☐	6. OBRANA	F	Rozesílání podvodných zpráv s cílem vylákat od uživatelů přihlašovací údaje.
☐	7. SPOOFING	G	Prohledávání online fór a hackerských kanálů kvůli ukradeným firemním datům.
☐	8. PHISHING	H	Uživatelská jména, hesla a soukromé tokeny používané k ověřování digitálních identit.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

1. Neoprávněné odhalení soukromých databází s osobními záznamy uživatelů. (5)

5. Druhý ověřovací krok (například hardwarové klíče) chránící přihlášení k účtům. (10)

6. Vytvoření falešného webu nebo e-mailu napodobujícího legitimní organizaci. (8)

7. Rozesílání podvodných zpráv, které z uživatelů lákají přihlašovací údaje. (8)

SVISLÉ NÁPOVĚDY

1. Uživatelská jména, hesla a soukromé tokeny k ověřování digitálních identit. (5)

2. Prohledávání online fór a hackerských kanálů kvůli ukradeným firemním datům. (10)

3. Omezení přístupu k úvěrovým záznamům proti podvodným žádostem o půjčky. (8)

4. Školení a technické kontroly používané k ochraně před krádeží identity. (6)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže.

VODOROVNÉ NÁPOVĚDY

1 vodorovně: Neoprávněné odhalení soukromých databází s osobními záznamy uživatelů. (5 písmen):

5 vodorovně: Druhý ověřovací krok (například hardwarové klíče) chránící přihlášení k účtům. (10 písmen):

6 vodorovně: Vytvoření falešného webu nebo e-mailu napodobujícího legitimní organizaci. (8 písmen):

7 vodorovně: Rozesílání podvodných zpráv, které z uživatelů lákají přihlašovací údaje. (8 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Uživatelská jména, hesla a soukromé tokeny k ověřování digitálních identit. (5 písmen):

2 svisle: Prohledávání online fór a hackerských kanálů kvůli ukradeným firemním datům. (10 písmen):

3 svisle: Omezení přístupu k úvěrovým záznamům proti podvodným žádostem o půjčky. (8 písmen):

4 svisle: Školení a technické kontroly používané k ochraně před krádeží identity. (6 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

Z	R	Y	Ě	Q	M	Č	P	Š	I	Ě	O	S	N	R
Y	R	E	Ó	Č	U	T	H	Ť	E	O	L	Í	B	A
G	B	J	C	P	Y	L	I	J	Y	B	L	Y	U	K
N	Ď	A	Ř	N	J	D	S	I	O	R	Ň	K	R	Q
I	F	D	Ň	Ň	M	Ř	H	S	T	A	U	Ť	Z	F
R	C	Ú	T	R	F	Ó	I	H	Š	N	B	V	M	D
O	T	Z	Ů	C	A	Ž	N	S	V	A	Ě	K	R	G
T	Ž	D	Ň	Ď	O	Ř	G	P	X	Q	C	Ú	A	B
I	A	Ž	O	D	V	L	A	O	Ď	Ó	Ď	É	Z	G
N	I	D	S	Ř	Ě	N	E	O	I	Š	Y	Ž	E	T
O	É	Ř	Ů	E	Ř	A	Á	F	Ř	K	P	O	N	Q
M	U	Y	R	J	E	S	U	I	I	Š	Č	Ň	Í	Ý
B	Ě	Š	X	W	N	Í	A	N	S	Ž	Ý	Ý	L	F
I	N	S	J	N	Í	M	Ú	G	Ť	P	G	R	Ř	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ý	Š	Ý	B	G	M	Ž	F

SEZNAM SLOV

ÚDAJE ÚNIKY MFAOVĚŘENÍ MONITORING ZMRAZENÍ OBRANA SPOOFING PHISHING

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. ÚDAJE**
- **B. ÚNIKY**
- **C. MFAOVĚŘENÍ**
- **D. MONITORING**
- **E. ZMRAZENÍ**
- **F. OBRANA**
- **G. SPOOFING**
- **H. PHISHING**

DEFINICE A POLE K PŘIŘAZENÍ

1. Rozesílání podvodných zpráv, které z uživatelů lákají přihlašovací údaje.
2. Uživatelská jména, hesla a soukromé tokeny k ověřování digitálních identit.
3. Vytvoření falešného webu nebo e-mailu napodobujícího legitimní organizaci.
4. Školení a technické kontroly používané k ochraně před krádeží identity.
5. Prohledávání online fór a hackerských kanálů kvůli ukradeným firemním datům.
6. Omezení přístupu k úvěrovým záznamům proti podvodným žádostem o půjčky.
7. Neoprávněné odhalení soukromých databází s osobními záznamy uživatelů.
8. Druhý ověřovací krok (například hardwarové klíče) chránící přihlášení k účtům.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. **JAÚED** _____

2. **NOMFVÍŘEĚA** _____

3. **AMZZEÍNR** _____

4. **ONGIFSPO** _____

5. **IYÚKN** _____

6. **NTIRIMOOGN** _____

7. **NOAARB** _____

8. **SHHGPNII** _____

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Věci, které je třeba udělat, když vám ukradnou identitu			
2	Věci, které byste neměli sdílet na sociálních sítích			
3	Věci, které si zálohujete			
4	Karty nebo doklady ve vaší peněžence			
5	Dokumenty, které byste měli chránit			
6	Co udělat po úniku dat			
7	Důvody, proč aktualizovat software			
8	Informace, které chce zloděj identity			
9	Zařízení, která lze hacknout			
10	Místa, odkud mohou uniknout vaše data			
11	Bezpečné návyky, se kterými můžete začít už dnes			
12	Známky toho, že je počítač nakažený			
13	Způsoby, jak prokázat, kdo jste			
14	Známky krádeže identity			
15	Varovné signály v e-mailu			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: OCHRANA PŘED ZNEUŽITÍM IDENTITY VEDENÍ FIRMY



Scénář: Významný člen nejvyššího vedení se stal terčem typosquattingových doménových jmen, která napodobují jeho osobní e-mail za účelem podvádění klientů. Navrhněte plán ochrany značky.

Otázka k diskusi: Analyzujte rizika podvržení značky a popište SPF/DKIM/DMARC a kontroly ověřování.

PŘÍPADOVÁ STUDIE 2: ÚNIK FIREMNÍCH PŘIHLAŠOVACÍCH ÚDAJŮ NA DARK WEB



Scénář: Databázový výpis z dark webu obsahuje několik set firemních přihlašovacích údajů patřících systémovým administrátorům podniku. Navrhněte strategii zmírnění.

Otázka k diskusi: Popište proces vyčištění přihlašovacích údajů a naplánujte nasazení správce hesel.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

4	13	26	1	21	30	8		14	6	8	20	30	14	30	32

35	15	4	8	11	1	17	30	22	26	22	35	39	19

22	35	10	27	8	20	15	19

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Co je krádež identity?

Trestný čin, při kterém útočník ukradne osobní záznamy (jako hesla nebo čísla sociálního pojištění), aby se za někoho vydával za účelem finančního zisku.

Q2: Jaká je nejčastější příčina krádeže identity?

Phishing je jedním z hlavních způsobů, jak zloději získávají hesla, lákáním uživatelů na falešné, podvržené weby.

Q3: Jak vícefaktorové ověřování (MFA) chrání identity?

MFA vyžaduje k přihlášení druhotný důkaz (například hardwarový klíč), a blokuje tak útočníky, i když vám ukradnou heslo.

Q4: Co je zmrazení úvěru?

Bezplatná služba blokující sdílení vašeho úvěrového souboru úvěrovými registry, která zlodějům brání sjednávat nové půjčky vaším jménem. [2]

Q5: Co je monitoring dark webu?

Software kontrolující hackerská fóra, zda neobsahují uniklé e-maily, hesla a osobní záznamy, a upozorňující vás, pokud jsou vaše data odhalena.

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Co znamená credential stuffing?

Automatizovaní boti zkoušejí uniklé seznamy hesel na stovkách webů, aby ovládli aktivní účty.

Q7: Proč je e-mailový spoofing nebezpečný?

Umožňuje útočníkům falšovat jméno odesílatele v e-mailech, takže phishingové zprávy vypadají, jako by přišly od důvěryhodných kolegů.

Q8: Jak správci hesel zastavují krádeže identity?

Ukládají složitá jedinečná hesla pro každý účet a odmítají automaticky vyplnit přihlašovací údaje na falešných phishingových doménách.

Q9: Co je spear phishing?

Vysoce cílený phishingový útok přizpůsobený jménem a údaji oběti, aby se zvýšila šance na oklamání.

Q10: Čím se úvěrové upozornění liší od zmrazení?

Výstraha říká věřitelům, aby před otevřením účtů ověřili vaši identitu, zatímco zmrazení zcela blokuje přístup k vašemu úvěrovému souboru. [2]

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak SIM swapping vede ke krádeži identity?

Útočníci přesvědčí pracovníky operátora, aby převedli telefonní číslo oběti na novou SIM kartu, a tím unesou 2FA kódy zasílané přes SMS.

Q2: Jaká je role DMARC v prevenci krádeže identity?

DMARC umožňuje vlastníkům domén blokovat podvržené e-maily, aby se nedostaly do schránek, a zastavit tak falešné e-maily napodobující firemní domény.

Q3: Proč je syntetická krádež identity obtížně odhalitelná?

Zloději kombinují skutečná čísla SSN s falešnými jmény a daty narození, aby vytvořili zcela nové kreditní profily a obešli základní upozornění na podvody.

Q4: Jak datoví makléři zneužívají osobní identity?

Makléři shromažďují veřejné záznamy, chování na webu a historie nákupů do profilových složek, které mohou uniknout nebo být prodány.

Q5: Proč je MFA přes SMS považováno za zranitelné?

Provoz SMS je zranitelný vůči zachycení, phishingu a SIM-swappingu na úrovni operátora.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Co je zámek úvěrového souboru?

Komerční služba podobná zmrazení, umožňující uživatelům okamžitě odemknout nebo zamknout svůj úvěrový soubor přes mobilní aplikaci.

Q7: Jak úniky firemních dat přiživují krádeže identity?

Uniklé databáze odhalují miliony přihlašovacích údajů v otevřené podobě a dávají zlodějům surová data potřebná k provedení cílených podvodů s identitou.

Q8: Jaké je riziko nadměrného sdílení na sociálních sítích?

Veřejné sdílení jmen mazlíčků, rodišť a rodných příjmení matky dává zlodějům odpovědi na běžné otázky pro obnovení účtu.

Q9: Jak biometrická přihlášení chrání profily identity?

Biometrie váže přihlášení na znaky jako otisky prstů nebo obličej; při uchování v zařízení se těžko kradou, ale uložená biometrická data mohou uniknout.

Q10: Jak pravidlo Red Flags bojuje proti krádeži identity?

Federální předpis vyžadující, aby finanční instituce vypracovaly písemné programy pro odhalování varovných signálů krádeže identity a reakci na ně.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

IdentityTheft.gov, provozovaný FTC, umožňuje obětem v USA nahlásit krádež identity a získat osobní plán obnovy. [1]

2. BEZPEČNOSTNÍ POSTŘEH

Hardwarové bezpečnostní klíče jsou MFA odolná proti phishingu, nejsilnější druh MFA, který CISA doporučuje. [4]

3. BEZPEČNOSTNÍ POSTŘEH

Kompromitovaná hesla jsou častým vstupním bodem při únicích dat a živí následné krádeže identity.

4. BEZPEČNOSTNÍ POSTŘEH

Zmrazení úvěru je podle federálního zákona zdarma a brání věřitelům v nahlížení do úvěrových souborů, dokud nejsou odemčeny. [2]

5. BEZPEČNOSTNÍ POSTŘEH

DMARC umožňuje vlastníkům domén přikázat poštovním serverům, aby podvržený e-mail, který neprojde kontrolami, odmítly nebo daly do karantény. [7]

6. BEZPEČNOSTNÍ POSTŘEH

SIM swapping umožňuje hackerům obejít dvoufaktorové ověřování přes SMS na bankovních portálech.

7. POSTŘEH K BEZPEČNOSTI

Podvody se syntetickou identitou kombinují skutečné a falešné údaje, takže je pro věřitele těžké je odhalit.

8. POSTŘEH K BEZPEČNOSTI

Mnoho lidí používá stejné heslo pro více online účtů, takže jeden únik jich může odhalit několik.

9. POSTŘEH K BEZPEČNOSTI

Datoví makléři sestavují podrobné složky o velkém počtu spotřebitelů, čímž vytvářejí koncentrované riziko pro soukromí.

10. BEZPEČNOSTNÍ POSTŘEH

Zotavení z krádeže identity může znamenat měsíce práce, jako je rozporování plateb a oprava úvěrových registrů.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů.

AKADEMICKÉ A OBOROVÉ REFERENCE

[1] Federal Trade Commission. (n.d.). IdentityTheft.gov: Report identity theft and get a recovery plan.

https://www.identitytheft.gov/

[2] Federal Trade Commission. (2025). Credit Freezes and Fraud Alerts.

https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts

[3] Federal Trade Commission. (n.d.). What To Know About Identity Theft.

https://consumer.ftc.gov/articles/what-know-about-identity-theft

[4] CISA. (n.d.). More than a Password.

https://www.cisa.gov/MFA

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[6] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.

https://pages.nist.gov/800-63-4/sp800-63b.html

[7] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 Otázka 1 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jakou primární metodu používají zloději identity ke krádeži přihlašovacích údajů? → Rozesílání falešných e-mailových upozornění, která uživatele přimějí zadat hesla na podvržených portálech

2 Otázka 2 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Jaká bezpečnostní kontrola poskytuje nejsilnější obranu proti únikům přihlašovacích údajů? → Vícefaktorová autentizace pomocí hardwarových klíčů

3 Otázka 3 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co představuje zmrazení úvěru? → Uzamčení úvěrových zpráv, aby zloději nemohli sjednávat neautorizované půjčky

4 Otázka 4 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Proč je monitoring dark webu užitečný? → Upozorní uživatele, pokud se jejich uniklé přihlašovací údaje objeví v nelegálních databázích

5 Otázka 5 — **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Co znamená sociální inženýrství? → Manipulace lidí, aby dobrovolně vyzradili důvěrné přihlašovací údaje

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Krádež identity může začít i offline, například ukradenou poštou nebo dokumenty.

7 **Otázka 7** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Vynucení MFA na všech osobních účtech blokuje většinu botových útoků typu credential stuffing.

8 **Otázka 8** — **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Zmrazení úvěru zastaví nové úvěrové kontroly, ale neovlivní vaše stávající účty.

9 **Otázka 9** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Správci hesel chrání uživatele před phishingem tím, že odmítají automaticky vyplňovat hesla na podvržených doménách.

10 **Otázka 10** — **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Phishingové e-maily často používají naléhavý jazyk, aby vyvolaly emotivní, rychlé reakce.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

H 1. PŘIHLAŠOVACÍ ÚDAJE	D 2. ÚNIKY	A 3. MFA	G 4. MONITOROVÁNÍ
C 5. ZMRAZENÍ	E 6. OBRANA	B 7. SPOOFING	F 8. PHISHING

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 PŘIHLAŠOVACÍ ÚDAJE	2 ÚNIKY	3 MFA	4 MONITOROVÁNÍ
5 ZMRAZENÍ	6 OBRANA		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 H – PHISHING	2 A – ÚDAJE	3 G – SPOOFING	4 F – OBRANA
5 D – MONITORING	6 E – ZMRAZENÍ	7 B – ÚNIKY	8 C – MFAOVĚŘENÍ

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy PŘIHLAŠOVACÍ ÚDAJE, ÚNIKY a MFA a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

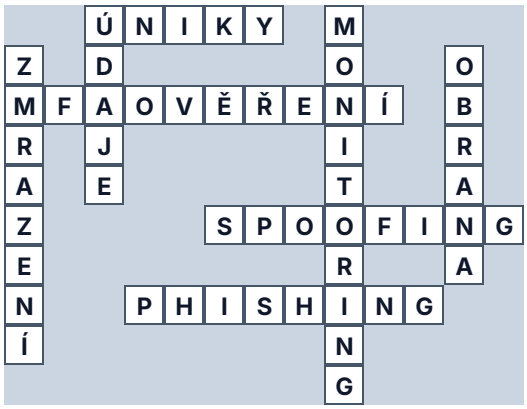
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

Z	R	Y	Ě	Q	M	Č	P	Š	I	Ě	O	S	N	R
Y	R	E	Ó	Č	U	T	H	Ť	E	O	L	Í	B	A
G	B	J	C	P	Y	L	I	J	Y	B	L	Y	U	K
N	Ď	A	Ř	N	J	D	S	I	O	R	Ň	K	R	Q
I	F	D	Ň	Ň	M	Ř	H	S	T	A	U	Ť	Z	F
R	C	Ú	T	R	F	Ó	I	H	Š	N	B	V	M	D
O	T	Z	Ů	C	A	Ž	N	S	V	A	Ě	K	R	G
T	Ž	D	Ň	Ď	O	Ř	G	P	X	Q	C	Ú	A	B
I	A	Ž	O	D	V	L	A	O	Ď	Ó	Ď	É	Z	G
N	I	D	S	Ř	Ě	N	E	O	I	Š	Y	Ž	E	T
O	É	Ř	Ů	E	Ř	A	Á	F	Ř	K	P	O	N	Q
M	U	Y	R	J	E	S	U	I	I	Š	Č	Ň	Í	Ý
B	Ě	Š	X	W	N	Í	A	N	S	Ž	Ý	Ý	L	F
I	N	S	J	N	Í	M	Ú	G	Ť	P	G	R	Ř	G
Ž	Á	Ó	Ů	Ě	Ú	C	Ý	Š	Ý	B	G	M	Ž	F

ŘEŠENÍ KŘÍŽOVKY



PRŮVODCE PRO VYUČUJÍCÍ K ŘEŠENÍ KŘÍŽOVKY

VODOROVNÉ NÁPOVĚDY

1 vodorovně: ÚNIKY Neoprávněné odhalení soukromých databází s osobními záznamy uživatelů. (5 písmen)

5 vodorovně: MFAOVĚŘENÍ Druhý ověřovací krok (například hardwarové klíče) chránící přihlášení k účtům. (10 písmen)

6 vodorovně: SPOOFING Vytvoření falešného webu nebo e-mailu napodobujícího legitimní organizaci. (8 písmen)

7 vodorovně: PHISHING Rozesílání podvodných zpráv, které z uživatelů lákají přihlašovací údaje. (8 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: ÚDAJE Uživatelská jména, hesla a soukromé tokeny k ověřování digitálních identit. (5 písmen)

2 svisle: MONITORING Prohledávání online fór a hackerských kanálů kvůli ukradeným firemním datům. (10 písmen)

3 svisle: ZMRAZENÍ Omezení přístupu k úvěrovým záznamům proti podvodným žádostem o půjčky. (8 písmen)

4 svisle: OBRANA Školení a technické kontroly používané k ochraně před krádeží identity. (6 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. JAÚED — ÚDAJE
2. NOMFVÍŘEĚA — MFAOVĚŘENÍ
3. AMZZEÍNR — ZMRAZENÍ
4. ONGIFSPO — SPOOFING
5. IYÚKN — ÚNIKY
6. NTIRIMOOGN — MONITORING
7. NOAARB — OBRANA
8. SHHGPNII — PHISHING

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"CHRAŇTE IDENTITU VÍCEFAKTOROVÝM OVĚŘENÍM"

Klíč k případovým studiím

A Případová studie 1: Ochrana před zneužitím identity vedení firmy

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Vysoce postavený manažer nejvyššího vedení je terčem typosquattingových domén napodobujících jeho osobní e-mail s cílem podvádět klienty. Navrhněte plán ochrany značky.
- Doporučená strategie a řešení: Zaregistrujte všechny běžné pravopisné varianty jména manažera. Nasaďte protokoly ověřování e-mailů (DMARC, DKIM, SPF) proti spoofingu domény. Vynucujte hardwarové MFA u všech firemních přihlášení nejvyššího vedení.

B Případová studie 2: Únik firemních přihlašovacích údajů na dark web

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Výpis databáze z dark webu obsahuje několik stovek firemních přihlašovacích údajů patřících systémovým administrátorům podniku. Navrhněte strategii zmírnění.
- Doporučená strategie a řešení: Proveďte celofiremní reset hesel. Nařiďte používání podnikového správce hesel. Vynuťte MFA na všech systémových portálech a nastavte průběžná automatizovaná upozornění z monitoringu dark webu.